Performance Work Statement
For
Defense Manpower Data Center
Defense Travel System (DTS) Information Technology Services
Order ID# ID03180017

1. INTRODUCTION

The Defense Manpower Data Center (DMDC) in support of the Office of the Under Secretary of Defense for Personnel & Readiness (OUSD P&R), Defense Human Resources Activity (DHRA) requires technical support services for the sustainment and maintenance of the Legacy Defense Travel System (DTS), referred to as the Defense Travel System and/or DTS within this PWS.

2.0 BACKGROUND

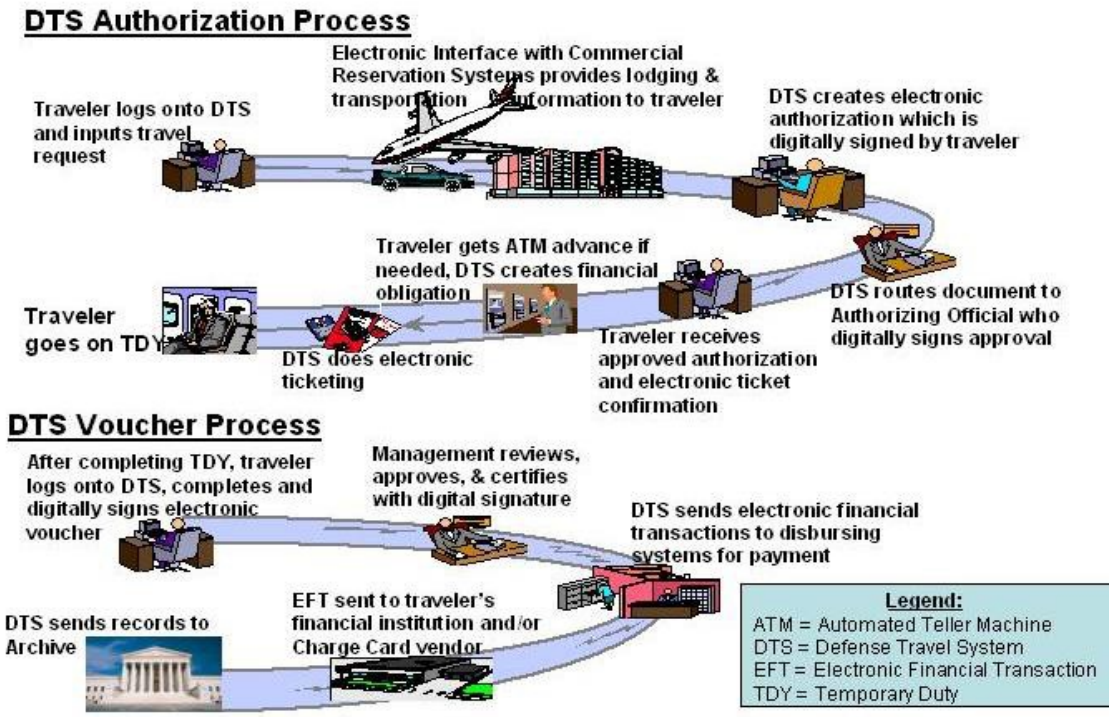
2.1 The Defense Travel System (DTS) is a fully integrated, automated, end-to-end travel management system that enables DoD travelers to create authorizations (TDY travel orders), prepare reservations, receive approvals, generate travel vouchers, and receive a split reimbursement between their bank accounts and the Government Travel Charge Card (GTCC) vendor. DTS operates at over 9,500 total sites worldwide. DTS services approximately 3 million DoD personnel, over 100,00 unique users access DTS on a daily basis, processes over 350,000 authorizations (travel orders) and 365,000 vouchers (requests for reimbursement) per month with the capacity to handle up to approximately 470,000 vouchers per month.

2.2 DTS resides on the DOD Non-classified Internet Protocol Routing Network (NIPRNet). DOD travelers access DTS using a web browser. Multi-factor authentication, access control and digital signature capability are enabled using DoD Public Key Infrastructure (PKI) certificates.

2.3 The Defense Manpower Data Center (DMDC) Program Management Office DTS (PMO-DTS) has program (acquisition, technical, operation and maintenance) oversight of DTS and the Defense Travel Management Office, OUSD (P&R) has functional oversight.

2.4 Travel Assistance Center (TAC)

The TAC provides travel assistance to the Defense travel community before, during, and after official travel. A team of analysts answer questions on a range of travel-related topics including DTS, DoD travel card, travel policy, commercial travel services and programs, and allowances and entitlements. The TAC is contracted through the DTMO and not part of this PWS. DTS business process flows are shown in the graphic below.



2.5 Information Technology & Network Environment

The following sections provide a general description of the current DTS operating environment. Complete lists of software and hardware configuration items shall be provided to the contractor as Government Furnished Equipment (GFE) and Government Furnished Information (GFI).

2.5.1 Hardware

The DTS hardware environment currently includes commercially available information technology and telecommunications equipment operating in a three-tiered architecture: a web tier, an application tier, and a database tier. Two production environments are in operation along with Development/Test environments:

- The primary production site is used to support production (normal system operation).
- The secondary production site provides system backup; operates as the Continuity of Operations (COOP) site; and is also partitioned to provide environments for training Government users and for testing new application software.
- The Development/Test environment is used for software remediation and development and testing of new software capabilities. This includes white box and integration testing of application software. The lab is currently located at the contractor facility.

Production hardware is currently located at commercial data centers in the National Capital Region. The hardware in these environments will be provided to the contractor as GFE. In the event that the primary production site is unable to operate normally, the secondary production site is used as a fail-

over COOP site to continue support of users. The databases between these two facilities are synchronized to prevent data loss.

DTS is requires a minimum of 98.5% operational availability (excluding Government-approved down time) of the primary site (measured 24x7x365 with maintenance periods limited to Government-approved downtimes), and a system performance requirement for an average web page response time of not more than two seconds during any hourly increment of any day. When the primary site switches over or fails over to the COOP site, (primary production site to COOP site) and, the COOP site is operating as the primary production site, the COOP site shall meet the same performance – operational requirements and metrics as the primary production site. Details pertaining to hardware environments and tools can be found in Appendix A.

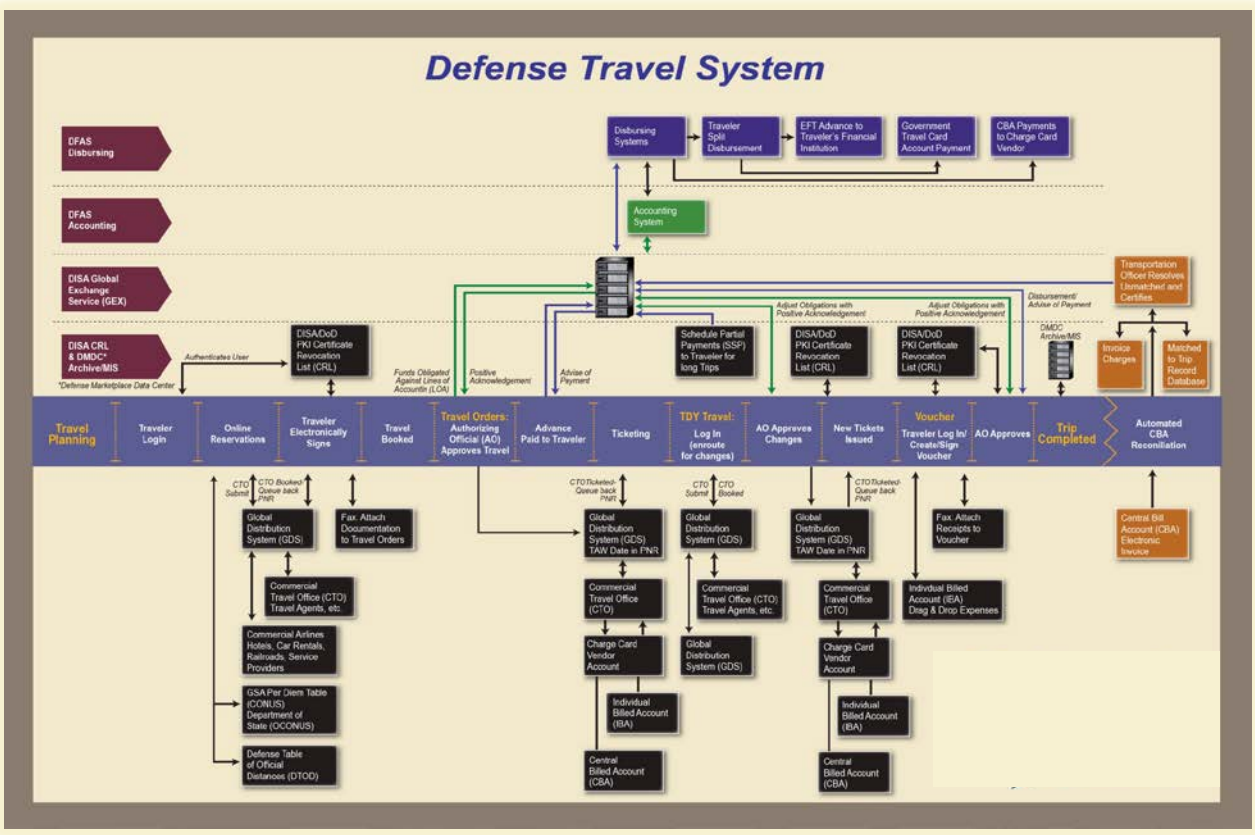
2.6 Software

DTS application software was developed and maintained under contract to the Government and the Government has unlimited rights and will be furnished in accordance with FAR 52.227-14, 252.227-7013 and 252.227-7014, along with associated documentation (such as requirements and design documents, version descriptions, and test specifications and results) to the contractor as GFI. The Transition plan documents required of the current Incumbent contractor will be provided to the contractor as they become available. Certain items such as network management tools and performance monitoring tools shall be procured and maintained by the contractor. (See Appendix B)

2.7 Network and Interfaces

Among the systems that interface with DTS to achieve required functionality are the following:

- Non-Classified Internet Protocol Router Network (NIPRNet) to provide worldwide access by users;
- Global Exchange (GEX) for interfaces with Government financial systems;
- Public Key Infrastructure (PKI) to determine currency and legitimacy of travelers' Common Access Cards (CAC);
- Defense Manpower Data Center (DMDC) for archiving of records;
- Government Charge Card Vendor (GOVCCV) for payment of charge card accounts;
- Global Distribution Systems (GDS) for availability and reservations.



For a list of network and system interfaces within DTS see Appendix C.

2.8 Three Tier Helpdesk (T3HD) Model

The DTS helpdesk employs a three-tier standard industry model for servicing DTS user problems. Oversight for the first two (2) tiers is managed by the DTMO and is not a requirement under this PWS. Oversight for the third tier is managed by DTS PMO and a requirement of this PWS.

Tier 3 (T3HD) support is the responsibility of the Contractor. T3HD staff is required to resolve all remaining detailed technical issues. Examples of these issues include coding defects; database or data object problems and system or hardware failures. These are expected to be technical issues that require examination and correction of code or data that is not otherwise accessible to T1HDs or T2HD. The process by which issues are currently escalated to the T3HD includes the capturing of the users work process when encountering the issue (via screenshots), a description of the problem, and an impact statement on behalf of the user. This information is compiled into a Software Problem Report (SPR).

2.9 Software Problem Report (SPR) Priorities

SPRs are categorized into the following priority levels and disposition is determined by the Governance Body. The Governance body consists of ad hoc members, as necessary, and may include the functional

sponsor, user representatives, program office personnel and the contractor. The contractor shall provide support to analyze the SPRs, provide feedback on the prioritories, and incorporate SPR resolution in its integrated master plan.

- Priority 1 (P1) - CRITICAL - Any problem that will prevent the system from being deployed, or, once deployed, will cause the system to be unavailable, or prevents the accomplishment of a mission-essential capability.
- Priority 2 (P2) - SERIOUS - Any problem that adversely affects or prevents a user from executing a mission-essential capability for which there is no acceptable workaround.
- Priority 3 (P3) - MODERATE - Any problem that prevents a user from executing a mission-essential capability, but has a government-approved**,** acceptable workaround.
- Priority 4 (P4) - MINOR - Any problem that presents operator inconvenience but does not affect the accomplishment of a mission-essential capability.
- Priority 5 (P5) - COSMETIC - Any problem or change that is merely cosmetic (typographical errors that do not change the meaning of an instruction or a message, a more descriptive error message, etc.).

The Travel Assistance Center (TAC) escalates 40-50 Potential Problem Tickets (PPTs) per month. Those tickets require analysis and testing in an effort to reproduce. Once reproduced, the PPT becomes a System Problem Report (SPR) and is ranked with the sustainment contractor, DTMO, DMDC, and the TAC to prioritize the fix in monthly releases. If not reproducible, regular meetings are in place to garner more information on circumstances, etc. There are 1000+/- tasks sent to the sustainment vendor for locked documents which are manually abandoned. This is a monthly clean up task which falls within Tier 3. There are also issues that require a "Permission Level 9 (PL9)" correction there are approximately 300+ per month. PL9s covers situations where a document is stuck or lost in processing, has never been received back from one of the financial systems or at the other end- DFAS, etc. There are routine reoccurring meetings with DTMO, the TAC, and the PMO to cover these situations and ensure proper communication is happening.

2.10 DTS LEGACY DISPOSITION

The Government plans to modernize travel modules within the legacy DTS system as implemented, the contractor shall, at government direction, de-commission the modules and support any necessary data migration work.

3.0 OBJECTIVE

The objective of this PWS is to manage and support the operation, maintenance, versioning and upgrade of the Defense Travel System throughout its entire lifecycle. The contractor shall include best practices, techniques and procedures essential to the applications operation, performance and efficiency. The principal objectives of performance under this PWS are stated below:

- Use existing GFE hardware and GFI operating system software for initial hosting of DTS.

- Manage and maintain the DTS system in two (2) production environments: the primary

production environment to operate the system; and COOP site (physically separate backup facility) for Disaster Recovery (DR), Continuity of Operations (COOP), load and performance testing, and end user training. Physical facilities for housing CDCs must be located in the contiguous continental United States. Equipment connected to the circuits shall be installed, tested, and successfully complete a DOD Risk Management Framework accreditation, obtaining and maintaining either an Authorization to Operate to Operate (ATO) or an Interim Authorization to Operate to Operate (IATO).

4.0 REQUIREMENTS

4.1 TASK 1 - PERFORM PROGRAM AND PROJECT MANAGEMENT & PLANNING

4.1.1 Develop and maintain a DTS Integrated Master Plan (IMP). The IMP is an event-based, top-level plan consisting of a hierarchy of Program Events. Each event shall be decomposed into specific required accomplishments and each specific accomplishment shall be decomposed into specific Entry and Exit Criteria. The IMP will include the status; statistics; risk management review; critical path; and other milestone progress checks and updates; as well as technical content review. Tasks from the final and Government-approved IMP shall be selected as milestones against which Contractors' progress is monitored. The IMP is an evolutionary document that shall be updated at least annually and identify tasks and deliverables specified in operating procedures that shall be completed by the contractor. Any updates to the IMP shall be incorporated to the order upon Government approval.

4.1.2 Develop and maintain a program-level Work Breakdown Structure (WBS) with dictionary to enable the decomposition of the work to be executed by the product/project teams to accomplish the product/project objectives and deliverables in accordance with Program Governance procedures and guidelines.

4.1.3 Develop and maintain a decision log to provide a concise, centralized record of all decisions, approvals or agreements affecting the scope, schedule, or internal and/or external deliverables for the project. The log shall be updated as needed and included with theIMP and schedule updates.

4.1.4 Maintain, refine, and revise the program collaboration sites on DMDC-approved collaboration platform. This would be the new DMDC Sharepoint or the Defense Information Systems Agency (DISA) Enterprise Portal Service (DEPS)Sharepoint implementation., as well as external locations when required. The DMDC internal site must include project overview documents; a consistently updated document library that preserves document history; schedules; dashboards; assignment and POC lists; summaries and agenda for all meetings and conferences attended; and support for collaborative editing/versioning of project documents.

4.1.5 Attend project meetings and conferences in support of DTS projects. The Government anticipates 2-5 meetings/teleconferences per week per project or application. Provide meeting summaries that reflect the meeting highlights, including a list of the issues discussed; any action items created and to whom each is assigned; and all decisions or determinations from the meeting and the decision makers for each.

4.1.6 Maintain, enhance, and revise all required project documentation, including project charters; concepts of operation (CONOPS); business requirements documents; integrated business use cases, user stories, and epics; functional designs and specifications; technical designs and specifications; file management policy; process flow and activity diagrams; and developer/technical use cases.

4.1.7 Coordinate with all DMDC governance bodies such as DMDC Information Systems Security Group (DISSG), Architecture Review Board (ARB), Enterprise Quality Assurance (QA), Configuration Management (CM), IT Operations, Consolidated Call Center (CCC), DMDC Management Advisory Group (DMAG), cybersecurity working group, production support, implementation support, and other impacted divisions for project requirements and execution.

4.1.8 Adhere to all DMDC Business Process Re-Engineering (BPR) workflows, requirements, and tool usage.

4.2 TASK 2 - CONDUCT DEVELOPMENT, MODERNIZATION & ENHANCEMENT (DME) TIME & MATERIAL)

Development/Modernization/Enhancement (DME) includes introduction of new or modified functionality or scope that requires the re-engineering and/or enhancement of an existing system, the re-platforming of a system to a new technical architecture, or the development of a new system. These services focus on designing, developing, integrating, and maintaining applications, tools, services, and other software to improve business and mission capabilities, and application effectiveness. DME includes trouble-shooting, repair of defects as specified on System Problem Reports (SPRs), supporting the resolution of Help Desk tickets, integrating the revised application software into the DTS environment, and designing and maintaining the logical architecture of the software and system. Modification of software shall be approved by the DTS PMO in accordance with the approved Configuration Management Plan. DTS application software shall be provided as Government Furnished Information (GFI).

4.2.1 Sustainment Services

Provide all phases of software maintenance as defined in ISO/IEC 14764. Possible categories are corrective maintenance, adaptive maintenance, perfective maintenance, and preventive maintenance.

4.2.1.1 Provide DTS application software sustainment and maintenance of all modified software to verify performance in accordance with requirements, and migrate tested and Government-accepted executable software to the hosting environment(s) for installation. These services may include maintenance, modifications, updates or additions to existing database tables, data objects and logical frameworks, servers, and middleware products, and configuration support for all such components. Sustainment services include:

- Analysis and correction of SPRs.
- Support resolution of TAC (“help desk”) trouble tickets received from the DTMO.

- Analysis and correction of application performance degradation.
- Full SDLC testing of application software patches and updates
- Add, modify, and delete functionality based on customer requirements
- Integrate new application architectures; improve application and tool quality and performance

4.2.1.2 Conduct migration support and oversight to the hosting environment for all newly installed application software products and components. Replace or upgrade any end of life components. Application software changes will be incorporated into DTS software maintenance releases to provide continual system improvement upon approval of the PMO. The DOD sustainment plan is for an average of four such maintenance releases per year, for changes to COTS software underpinning the DTS application.

4.2.1.3 Maintain application software, logical frameworks, middleware and server platforms and tools, data and storage management, and design and maintain logical architecture and software data structures (including newly developed capabilities) to be compatible with CDC 1 (production) and CDC 2 (COOP) environments

4.2.1.4 Maintain existing application software, middleware, frameworks, database, data objects, and perform ongoing defect and cybersecurity remediation and updates. Support planning and control of all system operations, capacity planning and maintenance activities.

4.2.1.5 Implement routine maintenance and installation of software and middleware products.

4.2.1.6 Monitor and support DTS databases data and objects and any applications of middleware associated.

4.2.1.7 Provide maintenance of applications to include analysis of problem reports, preparation of resource estimates and schedules to effect necessary changes, design and code changes, conduct testing of all changes, complete and/or update of all documentation affected by the required changes; and coordination of change implementation through appropriate approvals and user notifications.

4.2.1.8 Maintain logical component of system interfaces.

4.2.1.9 Provide, maintain, operate and support a software defect tracking tool, and electronic access for at least fifteen concurrent users. The tool shall, at a minimum, have the capability to include the following information about software defects, including SPRs: tracking number, title, description, priority, functional area, user impact, and proposed release to incorporate repair. The tool shall support the migration of existing remediation information.

4.2.1.10 Monitor and provide system administration and users' reports that include results from monitoring of system resource utilization, production log analysis, disk storage utilization, and identification of corrupt files or processes.

4.2.1.11 Maintain and manage software and updates for the Global Distribution System (GDS), OpenJaw, and Travel Industry (ITA) software and other logic components of the system, including detailed analysis of logs, system configurations and remediation of problems.

4.2.1.12 Maintain system stability of operation for both CDC 1 (production) and CDC 2 (COOP) systems (such as routine recycling of application and middleware components as required).

4.2.1.13 Support software interfaces and other logical components of the system to ensure transactional and archival integrity of all financial data and interface information.

4.2.1.14 Create and maintain a development and lab environment(s) to support source code and logic component remediation. The environment(s) shall provide the ability to test new code fixes, configuration modifications and updates or modifications to any logic components of the system and allow full integration testing in accordance with industry best practices. The environment(s) must include ability to test against a representative data set, simulate transactions and interface stubs.

4.2.1.15 Update and maintain a Requirements Traceability Matrix (RTM) that lists all system and component requirements and details how and where they are addressed in the system design.

4.2.1.16 Implement and maintain a Software Maintenance and Development Plan (SMDP) that defines the steps by which the development and maintenance of software will be accomplished, as well as the management approach to software development and maintenance. The SMDP shall address software processes, methods, organizational responsibilities, tools, configuration management, software quality, metrics, and other activities relevant to fulfilling the Performance Work Statement.

4.2.1.17. Relating to moderization, the contractor shall, at government direction, de-commission the modules and support any necessary data migration work.

4.2.2 Software Development Services (Enhancements)

Software development shall place emphasis on coding that is easily maintained, highly secure and compliant with DMDC coding practices. It is expected that the Contractor shall maximize and facilitate code re-use by leveraging already existing or project specific software re-use libraries. Executable and source software generated specifically for this task shall have all rights relinquished to the Government and, at the Government's discretion, be made available for other Government users to obtain.

4.2.2.1 Utilize Agile development methodologies, such as Scrum or Kanban to include sprint planning, application design, development and testing, deployment, sprint review, and sprint retrospective. Software development lifecycle shall focus on the repetition of abbreviated work cycles and functional requirements. Using this methodology, the Contractor shall manage all required activities including, but not limited to:

- Create user story

- Create acceptance criteria
- Develop automated test scripts
- Create design
- Write code components
- Create/update/run unit tests
- Create/update/run functional qualification tests
- Conduct code review
- Update master installation document
- Deliver Code with automated build capability
- Monitor integration tests
- Review acceptance by users

4.2.2.2 Support the change request (CR) process and upon Government request analyze and cost CRs.

4.2.2.3 Support the design and implementation of software CRs resulting from Public Law changes or DOD regulatory changes, organizational changes, system roles that impact workflow, and accounting system table changes for fiscal year crossover.

4.2.2.4 Analyze system engineering and architectural issues, lead efforts in planning, analysis, engineering review, improvement and integration of DTS architecture as relates to all software servers, frameworks, application software, middleware, and databases.

4.2.2.5 Develop logical components for system interfaces.

4.2.2.6 Support the creation of external connections to the reporting database, maintain and provide updates to the users' guide (at a minimum bi-annually) if development efforts, changes modifications, or expanded tool functionality/capability warrants.

4.2.2.7 Support the creation of external connections to the transactional database both production and test.

4.2.2.8 Maintain and create system artifacts that contain technical information such as the system design document and provide frequent (at a minimum weekly, as frequent as daily) updates to DMDC's tracking tool, Jira.

4.2.2.9 Provide a Software Version Description (SVD) for each version of production software at the Production Readiness Review (PRR) milestone.

4.2.2.10 Develop enhanced or new capabilities for application software, middleware, frameworks, database, and data objects.

4.2.2.11 Conduct peer code reviews and document the results via an electronic medium (e.g.,

Confluence, JIRA)

4.2.2.12 Conduct release planning to ensure streamlined, effective and productive communications and work products.

4.2.2.13 Maintain and support a code vault and versioning system, conduct code reviews and document the results in the Monthly Status Report (MSR).

4.2.2.14 Perform Configuration Management audits and identify configuration items throughtout the Software Development Lifecycle.

4.2.3 Software Testing and Integration

4.2.3.1 Software testing shall be performed in support of software development performed under PWS 4.2.1 and 4.2.2; create automated test cases, document testing methods, execute test scripts, capture test artifacts and record the results.

4.2.3.2 Create and maintain test environments for all application software and associated data environments. The application framework and logical servers shall emulate the production architecture. All development changes, new releases, fixes,and patches shall be tested. Create and maintain a test environment with external interfacing connections used for System Acceptance Testing. Changes made to any financial interfaces require end-to-end testing. Testing activities will vary in size, scope and duration. All development changes, new releases,system changes and fixes must be tested in a lab.

4.2.3.3 Testing shall include unit testing, integration level testing and remediation, followed by vulnerability, cybersecurity/Information Assurance (IA) compliance, regression and functionality testing before delivery to the DTS PMO for testing and acceptance. DTS PMO may perform any combination of integration, functional, regression and qualification test scenarios that support Government acceptance for production fielding of Sustainment and Maintenance Releases.

4.2.3.4 Create and maintain a Software Test Description (STD).

4.2.3.5 Create a Software Testing Report (STR) within ten (10) days of completion of contractor testing, all requirements in “IEEE/EIA 12207.1-1997 Lifecycle Data” subsections: 6.29 Test or Validation Results Report. Reference DoD DID DI-IPSC-81440A for further guidance.

4.3 TASK 3 – CONDUCT BUSINESS INTELLIGENCE AND REPORTING SERVICES

(PWS 4.3.1 to 4.3.14.3 are Optional after the Base Period)

4.3.1 Support the ingestion, data tagging, and management of data as a service model and the creation of external connections to the reporting database. This includes but is not limited to maintaining and developing the database, data objects and Business Intelligence (BI) tool and objects and Data Mart.

Maintain ETL and reporting performance in Production. Conduct performance testing for ETL and reporting changes to ensure timely updates to the data mart and positive end user experience. Manage queries and automated scripts in a source/version control tool that link to a task management tool, i.e. JIRA."

Provide control totals and document validation of ad hoc reports/data pulls in JIRA."

4.3.2 Update users' guide and data dictionary (at a minimum bi-annually); and develop reports and associated data elements to the data mart based upon new reporting requirements.

4.3.3 Perform capacity planning, ongoing tuning of the database instances and OBIEE reporting tool; plan and implement backups and recovery of the database and OBIEE reports. .

4.3.4 Enforce and maintain database constraints to ensure integrity of the database; administer all database objects, including tables, clusters, indexes, views, sequences, packages and procedures

4.3.5 Conduct impact analysis of changes made to the database objects; troubleshoot problems regarding the database, application and development tools. Implement quality control procedures, ensure data integrity and accuracy, and assist data analysts with responses to data inquiries.

4.3.6 Maintain data integrity; create dashboards, visualizations and analyses that surface insights and drive key business decisions. Provide data cleansing efforts to correct data quality issues.

4.3.7 Automate, test, and evaluate existing and new data file processes to include data loading and data processing processes and quality control reports. Track, log, monitor, and evaluate output statistics and transactional processing.

4.3.8 Analyze data, develop data extracts, identify trends, and create documentation and reports.

4.3.9 Develop and update DTS technical documentation. Documentation at minimum shall include:

- Updates: minor modifications to the system aligned with the production baseline.
- Deltas: significant modifications to the system, new documentation shall contain details describing only the changes, and shall align to the new production baseline.
- Baselines: a full documentation package is created that includes all previous deltas baselines and new changes.
- Root cause analysis reports: reports that analyze test or deployment failure

4.3.10 Create and maintain a requirements versioning tool, and provide electronic access for fifteen concurrent users. The tool shall, at a minimum, have the capability to migrate existing software requirements and respective versions.

4.3.11 Reserved.

4.3.12 Collect and analyze database statistics, events, availability, performance and trends; provide statistics in the monthly status report.

4.3.13 DTS reference tables are updated through the retrieval of data from email, FTP server, or web site. This process addresses the review and loading of retrieved data into the DTS production environment to ensure contents are up-to-date and valid.. The type of data updated includes Government-provided and commercial data including, but not limited to: Per Diem and Meals rates, preferred and Defense Lodging System (DLS) lodging data, FEMA hotel data, and closest airport data).

4.3.14 Recurring and Ad Hoc Reports

Ad Hoc reports may include, but are not be limited to investigative inquiries; Freedom of Information Act (FOIA) requests; Inspector General (IG), Government Accountability Office (GAO), supporting criminal investigations and other Government Agencies that request data.

4.3.14.1 Data pulls shall not take longer than five working days to complete; for more-difficult requests requiring more than than 5 days the contractor shall provide a delivery date within twenty-four for Government approval. In cases of national and weather emergencies, the Contractor shall be provide data within hours of receiving the request. Typical data that is required for these types of requests are a list of personnel within a set location area.

4.3.14.2 Support requests for recurring ad hoc data pulls and monthly reports. Reports shall be pulled from the existing database data or the archive database data. The Contractor shall be provided a list of all monthly reports that are recurring, but may have additional reports due on a case-by-case basis. Monthly data pulls shall be completed in three (3) working days. For larger data pulls the contractor shall provide a delivery date within twenty-four (24) hours after receipt.

4.3.14.3 Automate and document processes and procedures for current and future recurring reports (including those that are currently produced by government employees) so no human intervention is required. Utilize DMDC government-approved tools.

4.3.15 Compliance Auditing

4.3.15.1 Support and assist with preparation, and procedural guidance, for Federal Financial Management Improvement Act (FFMIA) assessments and reviews on the Investment Advisory Group system changes request and modernization packages.

4.3.15.2 Prepare a Compliance Audit Support Plan and support external auditing efforts relative to determining the system's compliance with federal laws, regulations and policies.

4.3.15.3 Support Financial Improvement and Audit Readiness (FIAR) efforts to include preparation of Statement for Standards Attestation Engagements (SSAE), financial audits, to meet the congressionally-mandated deadlines to achieve fully auditable financial statements.

4.3.15.4 Provide support and successfully complete initiatives; analyze current business processes and identify best practices for developing and maintaining compliant and auditable financial information. Support and assist with A123, Federal Information Systems Control Audit Manual (FISCAM) and Risk Management Framework audits. Develop and execute detailed audit readiness methodology, policy, and guidance; perform audit readiness assessments and provide recommendations on the effectiveness of Internal Controls (IC) and the status of the program.

4.3.15.5 Support data calls from auditors and provide documentation and demonstration of audit controls required to support DMDC application and systems control objectives. Evaluate and provide recommendations for the adjudication of Notification of Findings (NOF) and the development of Corrective Action Plans (CAP), which includes plans, method to manage resulting, identifying, tracking and verification of actions taken.

4.3.15.6 Provide system and financial documentation within agreed-upon timeframes and establish a common, detailed, understanding of the method for obtaining assurance. Assist in preparation of Assertion Packages to achieve audit readiness in accordance with DoD FIAR methodology and requirements. Perform analysis of business processes and internal controls to identify risks.

4.3.15.7 Provide recommendations to Government and external customers to improve client internal controls, accounting procedures, and financial statements. Identify and devise new or revised policies and procedures as well as business process improvements that address significant impediments to auditability.

4.3.15.8 Coordinate with external audit personnel to provide access, information, and demonstrate compliance with controls mandated for system compliance. The contractor shall provide information as needed in real-time or near real-time about system areas, which may have potential vulnerabilities/violations.

4.3.15.9 Support the Federal Information System Controls Audit Manual (FISCAM) audit working group questions and requests for vendor-generated documentation.

4.3.15.10 Deliver a software quality evaluation and performance review (SQPR) on the quality of the software in accordance with ISO 9126 and ISO/IEC 12207 for new developed application software within 30 days after software release of new system functionality. The evaluation of the Software Quality Performance Reports (SQPR) may include manual examination of the code and/or analysis using appropriate software tools, and may be done by a third party entity. This third party will be independent of this contract. However, the Contractor shall be required to meet with the third party entity and may be required to provide the source code and any other pertinent information which enables the third party entity to conduct an independent evaluation of the SQPR's.

4.3.16 Cybersecurity/Information Assurance (CYBER/IA) and IT Contingency Plan

All application deliverables shall meet the requirements of DoD Instruction 8500.01, Cybersecurity. Application deliverables should also meet Risk Management Framework (RMF) requirements set forth in Guide for Applying the Risk Management Framework to Federal Information System, SP800-37, Rev 1, DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), DoDD 8115.01, Information Technology Portfolio Management. Comply with technical certification and training as specified in Deparment of Defense Instruction (DODI) 8570.01-M Information Assurance Workforce Improvement Plan, through Change 4, of November, 2015.. (See Appendix F)

4.3.16.1 Develop and maintain an Systems Security Plan to assess and manage risk and coordinate with the Information Assurance Officer.

4.3.16.2 Evaluate and respond to Information Assurance Vulnerability Alerts (IAVA) and Bulletins. Apply best practices for tuning of overall system performance. Monitor system performance and make recommendations for improvement. Final approval for all IA tasks under this contract belongs to the Information Assurance Officer, Cybersecurity Branch. The contractor shall obtain final approval from Cybersecurity. All IA-related design decisions, including cryptography, authentication, access control, data transfer and storage, Need-to-Know (NTK), or other IA technologies, must be coordinated with and approved by Cybersecurity.

4.3.16.3 Implement, apply and maintain STIG configuration to all DTS assets. Deviations from STIG configuration setting must follow the DMDC STIG Deviation process and be approved by the Cybersecurity Division.

4.3.16.4 Maintain continuous monitoring of security posture to include supporting the deployment and operations of Cybersecurity Division monitoring tools: ACAS, HBSS, and ArcSight. Document and validate cybersecurity compliance using eMASS.

4.3.16.5 Provide a Plan of Actions and Milestones (POAM) for remediation actions that cannot be accomplished by the Cybersecurity Division assigned completion date.

4.3.16.6 Comply with Information Assurance Vulnerability Management (IAVM) patching on applicable assets (e.g.,workstations, servers, network devices). Develop and implement a patch management plan that will test and remediate vulnerabilities within the DoD timeline (currently TASKORD 13-067, which may be reviesed during performance). Vulnerabilities are completed for critical findings within 7 days of discovery, high within 21 days of discovery and medium and lows within 60 days of discover according to TASKORD 13-067. Remediation shall follow DoD and DMDC IAVM guidelines. Report IAVM patch compliance to the Cybersecurity Division.

4.3.16.7 Ensure DTS assets have the required cybersecurity monitoring tools (e.g., tripwire agent, HBSS agent) installed and operational in accordance with DoD and DMDC policy. Provide all security logs to the DMDC logging solution.

4.3.16.8 Comply with security investigations for privileged users as stated in DODI 8500.2, E3.4.8 DoDI and in accordance with guidance provided by DoD.

4.3.16.9 Notify DMDC of any security incident within one hour of the incident and assist with the investigation.

4.3.16.10 Provide a IT Contingency Plan referencing NIST SP 800-34, Rev 1, Contingency Planning Guide for Information Technology Systems.

4.3.17 Software Engineering

4.3.17.1 Conduct software engineering studies and analyses so as to create an evolutionary plan for DTS. Objectives of improvements may be in the areas of maintainability, performance, reliability, extensibility, scalability, functionality, usability, or quality of developed code.

4.3.17.2 Provide all required design and development documents and supporting architectural documentation in compliance with the latest Department of Defense Architectural Framework (DoDAF) Enterprise Architecture guidance, described at: http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf.

4.3.18 Engineering Change Proposals (ECPs)

Provide Rough Order of Magnitude (ROM) estimates for ECPs to the DTS PMO to assist funding preparation at the service/agency level. A request for a technical proposal will be submitted by the DTS PMO representative to include detailed technical approach and more accurate estimate on level of effort required to complete the change. Responses to ECPs shall be submitted in accordance with procedures on Appendix D. . The ECP shall contain a sufficient description of the proposed change so that the Government Change Control Board (CCB) can make an informed decision on whether to proceed with the change. Once an ECP is approved by the government all drawings and diagrams required for the various technical documents and impacted by the ECP shall be updated. The diagrams shall adhere to the Department of Defense Architectural Framework (DODAF) standards.

4.3.19 Interface Engineering and Development

The following sections provide guidance on technical documents required to maintain accurate documentation of the DTS application and infrastructure.

4.3.19.1 Interface Requirements Specification (IRS)

Deliver an Interface Requirements Specification (IRS) for every interface development effort pursuant to an FRD (or equivalent). The IRS shall be delivered within 30 days of a Production Readiness Review (PRR) milestone for new development activities. See DoD Data Item Description (DID) DI-IPSC-81434A for further guidance.

4.3.19.2 Interface Design Description (IDD)

4.3.19.2.1 Maintain, modify and develop interfaces and related documentation. The government provides oversight and review of the results of the contractor's efforts through the PMO DTS test group.

4.3.19.2.2 Deliver an IDD after completing any interface development or modification. The IDD shall be delivered within 30 days of a PRR milestone for new development activities. See DoD DID DI-IPSC-81436A for further guidance.

4.3.20 Engineering Documentation for DTS Information Assets

The following sections provide guidance on technical documents that are required to maintain accurate documentation of the DTS application and infrastructure.

4.3.20.1 Software Product Specification (SPS)

Submit the updated Software Production Specification (SPS) for releases with new development or content changes. An updated SPS is required at the PRR In cases where other documents contain duplicate information , the contractor shall identify what document contains the required information and incorporate the information in other documents by reference. The referenced document shall reflect the most current production baseline. The SPS contains or references the executable software, source files, and software support information, including "as built" design information and compilation, build, and modification procedures for a CSCI. The SPS shall be delivered within 30 days of a PRR milestone for new development activities. See DoD DID DI-IPSC-81441A for further guidance.

4.3.20.2 System/Subsystem Specification (SSS)

For each new software release, (excluding SPRs) the Contractor shall deliver a System/Subsystem Specification (SSS), the SSS shall include flow control diagrams for internal system and provide traceability between the Configuration Items and the DTS System Requirements, including traceability of DTS System Requirements to Defense Travel Policy and Business Rules. The SSS shall comply with all requirements in IEEE/EIA 12207.1-1997 Lifecycle Data subsection: 6.26 System Requirements Specification. If any of the information is found in other documentation required by the PWS, that requirement shall be incorporated by reference to the other document providing the referenced document is up to date, per the current production baseline. The SSS specifies the requirements for a system or subsystems and the methods to be used to ensure that each requirement has been met. The SSS shall be delivered within 30 days of a PRR milestone for new development activities.

4.3.20.3 System/Subsystem Design Description (SSDD)

Provide a System/Subsystem Design Description (SSDD), describing the overall system and subsystem architectures needed to implement the DTS functional capabilities. It shall include system and subsystem component level architecture with sub and external system interface specifications using deployment diagrams, collaboration diagrams and sequence diagrams. The SSDD shall comply with the requirements in IEEE/EIA 12207.1-1997 Lifecycle Data; subsections: 6.25 System Architecture and

Requirements Allocation Description; 6.3 Concept of Operations Description and be delivered within 30 days of a PRR milestone for new development activities.

4.3.20.4 Database Design Description (DBDD)

Provide a Database Design Description (DBDD), in accordance with the requirements in IEEE/EIA 12207.1-1997 Life cycle Data, subsections: 6.4 Database Design Description. In the event this standard conflicts with this PWS the PWS shall prevail. The DBDD describes the design of a database, that is, a collection of related data stored in one or more computerized files in a manner that can be accessed by users or computer programs via database management system (DBMS). The DBDD shall be delivered within 30 days of a change to the database architecture .

4.3.21 Release Notes

Deliver Release Notes for each software release (including SPRs); documentation shall be a supplement to the above documents and shall detail the functional changes impacting the user community. Associated technical changes that may impact the user community shall be included as well. The Release Notes shall contain a cross-reference of changes to the requirements management tool (i.e., JIRA) using the requirements identification numbers. A draft of these release notes shall be available to PMO for review at the start of testing and shall be finalized prior to implementing the release in production. Release Notes shall be available to the user community when the release is implemented and will be distributed through DTMO/TAC existing channels. Release Notes shall be labeled by both the common release name and the designated number for the release and a mapping of release name to number shall be maintained by the contractor. A repository of the Release Notes shall be maintained for future reference by the DTS PMO.

4.3.22 Helpdesk Support

4.3.22.1 Provide Tier 3 Help Desk (T3HD) support. This shall include but is not limited to: resolving advanced problems relating to data or database issues, software defects, interface issues, or other system related problems that range from hardware and networks through software and supporting frameworks.

4.3.22.2 Directly support all helpdesk activities through in-depth analysis of system components (logical and physical) in a testing environment, develop a get well plan and implement the plan upon approval of the Government. Additional technical support activities may require direct contact with the T1HD and T2HD levels for user assistance support. Provide Tier 3 statistics in the monthly status report.

4.3.23 Maintain the DTS Operations Plan, the plan shall address:

- What is required to run operations out of either CDC facility
- Availability
- Responsiveness
- Hours of support

- Scaling and Obsolescence process
- Tools used

4.4 TASK 4 - SUPPORT DLA GLOBAL EXCHANGE ( ) TRANSACTION SERVICES

4.4.1 GEX Integration and Testing Support

4.4.1.1 Provide logical and physical mappings details on existing data transformation requirements and conduct unit testing of modified physical maps.

4.4.1.2 Assist in drafting and reviewing of change proposals (CPs).

4.4.1.3 Support DTS testing as it relates to existing partner systems, support for new systems shall be evaluated to determine if an ECP is required.

4.4.1.4 Maintain the GEX test platform with 80% uptime including test connection configuration/verification for DTS test events.The GEX platform includes support to existing partner system interface test activities with Government-provided test data and test scenarios.

4.4.1.5 Generate user accounts and support security protocols for the test platform and troubleshoot connectivity issues.

4.4.1.6 Conduct point-to-point (P2P) testing including scenario and test data for existing partner systems and support system qualification testing (SQT) conducted by the DTS PMO correcting rect mapping bugs, deficiencies or changes in requirements shall be elevated by ECP.

4.4.1.7 Participate in daily DTS PMO test meetings such as hot washes and Test Review Board (TRB).

4.4.2 Production Deployment and Support

4.4.2.1 Troubleshoot production connectivity issues, maintain and coordinate changes for IP addresses and username/password changes.

4.4.2.3 Support release upgrades, partner system software/middleware changes of existing interfaces.

4.4.2.4 Coordinate the restage of data when an issue arises that prevented the data from being posted successfully by a partner system, or DTS.

4.4.2.5 Research translation issues or failures which may result in map changes.

4.4.2.6 Maintain interface deployment guides (IDG) and support discussions of systems migrations from one database to another.

4.4.2.7 Generate, test and deliver production map updates and shared libraries to DMDC Transaction Services GEX.

4.4.3 Reserved

4.4.4 Analysis Support

Coordinate with the DT PMO to provide:

- Engineer Change Proposals (ECPs) in response to Functional Requirements Documents (FRD) and Change Proposals (CPs), or equivalent, for enhanced, modified or new software capabilities.
- Project meeting participation such as technical and status meetings as requested by the DTS PMO.
- Support the Fiscal Information System Controls Audit Manual (FISCAM) audit working group questions and requests for vendor generated documentation.

4.5 TASK 5 - CONDUCT HOSTING SERVICES

DTS production and failover environments are currently hosted at commercial data centers in the National Capital Region.

DTS requires warm failover capabilities. “Warm” means activities related to failover must be completed within 24 hours.

4.5.1 Hosting Migration

In the case where the contractor has to change the physical location of the data center(s) to another commercial location, the contractor shall:

4.5.1.1. Provide a Hosting Migration Plan (Preliminary and Final) for the physical movement of the data center(s). The plan shall reflect a series of specific test events with measurable and verifiable success criteria identified for each step, to ensure DTS transition is fully operational and ready to service DTS user community web traffic. The Hosting Migration Plan must address, at a minimum, the areas below and incorporate the process and sequence details for moving COOP and PROD sites:

- Conduct migration activities with third party equipment vendors to complete the installation of the DTS equipment.
- Perform migration during periods of low user activity such as weekends with the system being unavailable for no more than 72 hours.
- Facilities preparation, power, fire suppression, security, environmental, space plan, cabling/wiring, rack layout etc.
- Physical server and network architecture that is fault tolerant.
- Inventory control of the GFE.
- Installation details of Servers for the Web and Application Tier with High

Availability/failover & system redundancy details.

- Installation details of Data Tier Server, primary storage disc arrays, secondary storage, Primary Rate Interface (PRI) server and peripherals.
- Network Installation to include: NIPRNet circuits and related hardware, site-to-site communications, T1 / facsimile lines, VPN equipment, firewalls, and switches. Include test/validation time for these circuits/devices.
- Installation and testing of all required Interfaces.
- Internet/DNS Registry & Protocol Management.
- Risk identification and mitigation planning for each step of the process using the Contractors Risk Management process.
- Management and oversight responsibilities with contact details.
- Milestones and critical success factors with demonstrable criteria.
- A separate test plan for each move (CDC 1, CDC 2 and an integrated test for the full operational profile)
- Cut over plan for each move and a final cut over plan with acceptance criteria for full operational mode.
- A detailed list of all substituted components, if any, and a recovery statement that includes a secure location, point of contact, and scheduled times the Government can recover the unused GFE components.
- The process and sequence details for moving COOP and Production (PROD) sites.

4.5.1.2 Physical relocation of GFE from its current location to the new hosting site should be completed without delay, but the Government allows three months for the contractor to make the data center at the new location operational. If both data centers require relocation, to mitigate risk, the CDC 2 site shall be initially moved, followed by the CDC 1 site. Once NIPRNET connectivity is complete, the first set of GFE will be moved from CDC 2 to the contractor backup site; Contractor shall accept GFE and manage installation in their facility. If relocation is performed during transition-in period, the incumbent Contractor on the precedeing order shall be available to provide any technical support for transfer and installation as required. The contractor performing under this Order must conduct and obtain full DOD IA security accreditation at the new sites; this process may take up to sixty (60) days before the site is certified and ready to “go live.” After the first site goes live, the GFE move process will be repeated for moving CDC 1 hardware to the contractor’s second site. GFE shall include, but is not limited to web servers, application servers, database servers, routers, load balancers or other network components, operating systems, software tools, utilities and other software to operate system hardware.

4.5.1.3 Disable the database synchronization, the primary storage disc arrays and power down CDC 2. The DTS PMO will oversee system transfer to the contractor’s backup site, and the Contractor shall install, test, then power up CDC 2, sync the transactional data/disc arrays and cutover system production to CDC 2. Moving, testing and syncing for CDC 1 follows, with production operations switching back to CDC 1 and backup environment restored in CDC 2. A maximum of seventy-two (72) hours of total and continuous non-availability is allowed during the final reconfiguration for CDC 1 (production) and CDC 2 (COOP).

4.5.1.4 Installation of NIPRNet circuits requires that hosting services include designing physical architecture of system and networks; providing all necessary computer networking and telecommunication hardware not supplied as GFE; providing all software not supplied as GFI required for operating systems, network operations and management; providing any other commercial, non-application software needed to enable operation of DTS; and maintaining all hardware support service agreements and all software licensing agreements. Government will provide line connections for NIPRNet.

4.5.2 Movement of Data Center to DISA DECC

Since this order has a potential life span of five years, changes in operations and capabilities are anticipated. DMDC is in the process of readying workloads and applications to migrate to a Defense Enterprise Computing Center (DECC). The Contractor shall provide services to support the desired outcomes, including:

- Comprehensive analysis and understanding of the current environment
- Comprehensive planning for migration that supports cost-effective, secure, and agile IT management
- Successful and complete transition of specified applications, solutions, and services
- Consolidated and simplified application, service management and monitoring to support cost-effective, secure, and agile IT management
- Successful decommissioning of specified hardware, applications, solutions, and services

In an effort to increase Information Technology (IT) efficiencies, lower risk and increase the probability of success with the computing platform, DMDC has decided to migrate DTS hosting to a Defense Enterprise Computing Center (DECC) at a point to be determined during the performance of this PWS.

Under this model, DISA will provide, manage, and administer the hardware and operating environments, and DMDC will continue to provide though this PWS, application and database support. The DISA model is DISA Capacity Services (CS), which is a form of Infrastructure as a Service (IaaS). The contractor is expected to support the migration of DTS data to the DECC hosting facility and provide a migration plan.

The required services include IT support for all DTS applications and products across in compliance with all associated DTS policies, processes, and procedures. The Contractor shall provide planning, technical coordination, and operations support prior to, during, and after the efficient and successful migration of all DTS systems to DECC. The contractor will not physically perform the actual hardware, network, and operating system related migration tasks. DISA will perform all the hardware, network, and operating system related tasks. Prior to, during, and after migration, the Contractor shall support all related system lifecycle activities and documentation that will be required as a result of the significant architecture and design changes the migration will cause.

4.5.3 Operational Availability Requirements

4.5.3.1 Operational availability shall be a minimum of 98.5%, measured 24x7x365 with maintenance periods limited to Government approved downtimes. Documentation of system operational availability shall be reported on a periodic basis. Operational availability requirements apply to both Production and COOP systems. Downtime approvals are issued by the Government for routine and emergency maintenance of the system and its physical and logical components, upgrades to the software or hardware components of the system, and for testing, when such testing requires making DTS unavailable to the users.

4.5.3.2 Provide a schedule for all downtime events. Approved downtime shall have Government approval and not affect performance metrics.

4.5.4 System Performance Requirements

Maintain an average web page response time of not more than two (2) seconds during any hourly increment of any day for the production system. Metric shall be measured inside the DTS firewall monthly. Documentation of system performance shall be incorporated into the Monthly Status Report.

4.5.5 Performance Tuning

4.5.5.1 Monitor the performance of physical and logical components of the system to include all operational metrics such as central processing Unit (CPU), memory consumption, network bandwidth and server request/reply response times, and any other customary system parameters as is normal in commercial best practices for the contractor's hosting operations utilizing ISO 9001:2008. Report Daily.

4.5.5.2 Tune or adjust the system components to meet the minimum system requirements at least once yearly and provide a report within one week of the tuning and provide recommendations for system performance improvements.

4.5.6 System Backup

4.5.6.1 Conduct backups of all data, software operating environments, configurations for those environment(s) and machine readable application code after any incremental change. Provide any other electronic files, software, or other items necessary to restore environments to an operational status. Backups shall be delivered in a machine-readable electronic media or file transfer within one week of backup to Iron Mountain.

4.5.6.2 Notify the Government of changes to configuration of hardware, architecture or other contractor-owned or leased software, via electronic means, within one week of change.

4.5.7 Configuration Management (CM)

4.5.7.1 Implement and maintain a hosting configuration management plan (CMP) for recording, tracking and reporting the configuration items (CI) for systems in development, include the baseline configuration of the platforms, systems, subsystems and apply Configuration Management (CM)

techniques that establish and maintain the integrity of the system, collect, review, track and archive Configuration Control Documents and support Configuration Control Boards

4.5.7.2 Maintain a code vault to manage source and executable software, configurations and configuration management information. Support transition of executable software and configuration artifacts and data objects to the CDC1 and CDC2 hosting environments. The Contractor's code repository shall be compatible with the existing versioning scheme.

4.5.7.3 Maintain software units through a version control system, using existing established version designations, in order to maintain baseline integrity within all baselines.

4.5.7.4 Provide traceability developed software units to the software configuration items that make up the DTS.

4.5.7.5 Update Bill of Materials (BOM) of architectural drawings, interface diagrams, as well as any associated systems specifications and requirements documents. DT PMO will approve all new hardware items to assure National Information Assurance Partnership (NIAP) compliance. Once approved hardware is integrated into the DTS, update and submit a network diagram reflecting any change.

4.5.7.6 Maintain all licensing, hardware support, and related agreements for all GFI and GFE; ensure GFE is upgraded and/or replaced in accordance with the Government approved Configuration Management Plan. The Contractor shall not make substitutions for hardware or software that is not in accordance with the Government-approved Configuration Management Plan.

4.5.8 **Configuration Audit**

4.5.8.1 Maintain the Configuration Audit Plan (CAP) with information required for conducting Functional Configuration Audits and Physical Configuration Audits. Reference MIL-STD-973 and MIL-HDBK-61A for guidance.

4.5.8.2 Identify the Hardware Configuration Items (HWCIs) to be audited identified by nomenclature, serial number, and/or any other applicable identifiers.

4.5.8.3 Identify the Computer Software Configuration Items (CSCI) to be audited by software title, code identification number, software inventory numbering system, and/or filename.

4.5.8.4 Provide a summary of the hardware and software requirements to be audited and outline the proposed audit procedure for each item.

4.5.8.5 Identify proposed milestones for the audit(s), conduct the audit(s), and provide the results of each audit to the Government.

4.5.9 Rollback Plan

Create and deliver a Rollback Plan. The plan shall detail if, when and how to revert to the old system if implementation fails, overview, milestones, roll back activities, resources and communication.

4.5.10 Disaster Recovery, COOP, and Contingency Planning

4.5.10.1 Provide adequate geographic separation from the primary production location for the backup production (COOP) ensuring the physical separation of the sites does not jeopardize the requirement for 0% data loss during a system switchover or failover.

4.5.10.2 Conduct risk analysis on the vulnerability of the COOP site to the same disaster event as one anticipated to occur at the primary production site (e.g., seismic, weather-related, terror attack or power grid failures etc.) and also describe the technical approach for ensuring 0% Approved Transactional data loss upon switchover or failover.

4.5.10.3 Conduct a COOP exercise or assessment that demonstrates a switchover or failover to the COOP site, and provide an after action report.

4.5.10.4 Provide a Disaster Recovery Plan.

4.5.11 Reserved

4.5.12 Hosting Transition Out Planning

The Contractor shall provide a Hosting Transition-Out Plan to transition DTS application Hosting services. The transition may be to a follow-on contractor or a Government entity. Unless hosting is earlier moved to the DISA DECC, It is anticipated that the Hosting Transition-Out would occur at the end of Option Year Four (4) (should all four options be exercised), with a period of performance not to exceed nine (9) months to complete final transition.

Significant knowledge transfer will likely be required to complete a seamless transition to a new Hosting entity. The Contractor's plans must reflect an approach that transfers required knowledge without divulging any proprietary information, and ensures a successful transition, with no more than seventy-two (72) hours of production downtime before establishing full operational capability at the new hosting facility.

Detailed requirements and time required to execute Transition-Out may vary depending on the Contractor's operational concepts and specifics of hosting environments at the time of transition.

Four (4) months prior to transition, the contractor shall provide a transition plan for CDC 1 and CDC 2 migration to a new contractor with all the activities and tasks required to maintain and sustain all the hardware and related operating systems software for both CDCs.

4.5.13 Operational Hosting Services

The contractor shall perform the following specific tasks:

4.5.13.1 Maintain the computing environment to achieve and sustain performance and availability requirements as stated in the following sections: Operational Availability Requirements, System Performance Requirements, and Performance Tuning.

4.5.13.2 Manage network connections to the established end points of demarcation. As per common business practices, hosting services involve layers 1, 2, 3 and 4 of the Open Systems Interconnection Model used by industry. (The sustainment and development services involve layers 5, 6 and 7.)

4.5.13.3 Manage and maintain the operating system software and the general operating environment.

4.5.13.4 Manage and maintain all third party software including patches and upgrades from the appropriate vendors. Manage upgrade activities and third party license issues as they pertain to the system environment.

4.5.13.5 Perform the duties as Oracle Database Administrator (DBA) for the database (DB) server administration and data synchronization.

4.5.13.6 Perform any other action in accordance with standard practices and operating procedures to maintain system performance and availability requirements.

4.5.13.7 Monitor system performance testing and final stage functional testing on the backup site to assure newly developed code, data structures and frameworks comply with performance specifications before release to the production system.

4.5.13.8 Manage, plan, advise, and implement system capacity, scaling, and obsolescence details and activities, including system component end-of-life issues.

4.5.13.9 Collect and review operational and system performance metrics as required ensuring service delivery requirements are met, see QASP. Report Daily.

4.5.13.10 Reserved.

4.5.13.11 Maintain, modify, update, and submit DTS documentation. Documentation will be submitted in electronic format.

Decisions on operational issues, all non-availability periods, software migrations, release schedules, system upgrade and changes, and any related risks assumed by the Government will be made by the PMO. As directed by the Program Manager for the DTS effort, designated personnel that support the

DTS, shall have access to the contractor facilities. In no case shall contractor deny the Government access to inspect contractor's facilities. This includes the production environment (CDC 1 and CDC 2) and the testing and lab environment.

Government requires multiple data points/metrics provided at varying intervals in order to ensure effective program management of the DTS. These data points/metrics consist of real-time, regularly scheduled, and ad hoc DTS performance information. The Contractor shall provide additional operational metrics, as required and consistent with standard industry practices, to the Government.

4.6 TASK 6 - SUBMIT REPORTS & DOCUMENTATION

Provide initial draft(s) of, and update, recommendations, for Government approval, project and organizational Standard Operating Procedures as changes in processes and procedures occur.

4.6.1 Monthly Status Report (MSR)

Submit a MSR for the previous month to the DMDC Contracting Officer Representative (COR), the GSA COR, GSA's IT Solutions Shop (ITSS) and to a designated area in SharePoint by the 15th calendar day of each month. The Contractor shall prepare an agenda and meeting minutes in a clear, concise and orderly manner. Briefing materials shall be made available to all attendees prior to time of briefing. The report should include data of sufficient detail to monitor the completion of work products against progress as documented in the PWS:

- Order Summary
- Performance metrics
- Schedule
- Up to date Integrated Master Plan
- Milestones achieved or missed
- Open Issues/Risk and mitigation Action
- Summary of Issues Closed
- Projected Activities
- Summary of accomplishments for each project
- Issues and Risks with impact and mitigation
- High Level Summary
- Percent of Work Completed
- Transaction Analysis Report data
- Data File Reporting data
- Data request reporting
- Error Pattern Reporting
- Database statistics, events, availability, performance and trends
- Tier 3 help desk statistics

4.6.2 Communications Plan

Develop and deliver a Communications plan that provides methods, timing, roles, responsibilities and key messages. The Communication Plan will describe how the contractor will establish a reliable means of communicating status about the contract to all appropriate stakeholders. It describes what needs and how it will be communicated, who is responsible for communicating with whom and when the communication needs to take place.

4.6.3 Problem Notification Report (PNR)

Submit a Problem Notification Report (PNR) to the Task Order Client COR, with a copy to the GSA CO/COR, within three days of the contractor encountering a problem or risk event that significantly impacts the cost, schedule, or performance of the Order (or any deliverable or project under the Task order). All PNRs must be tracked in the monthly status report (MSR) and through in-progress reviews (IPRs) until the Government agrees they are resolved. The PNR shall include, but not be limited to, the following:

1) Nature and sources of problem
2) COR was verbally notified on: (date)
3) Is action required by the Government? Yes or No
4) If YES, describe Government action required and date required
5) Will problem impact delivery schedule? Yes or No
6) If YES, identify what deliverables will be affected and extent of delay
7) Can required delivery be brought back on schedule? Yes or No
8) Describe corrective action needed to resolve problems
9) When will corrective action be completed?
10) Is increase cost to the Government anticipated? Yes or No

4.6.4 Meetings, Telephone Conferences & Trip Reports

Participate in telephone conferences and meeting to discuss on-going technical performance and problems. These calls are used to summarize activities that have been performed since the previous call and discuss the status of activities going forward. The contractor shall attend additional meetings as specified by the Government and provide meeting summaries. Participate and contribute to various agencies technical meetings to include Technical Working groups and various ad hoc technical tiger teams. Trip reports will be fully documented within five duty days of return for Government review. Trip reports will be provided for all conferences, IPRs, and travel.

Attend project meetings and conferences in support of various projects. The Government anticipates 2-5 meetings/teleconferences per week per project or application. Provide meeting summaries that reflect the meeting highlights, including a list of the issues discussed; any action items created and to whom each is assigned; and all decisions or determinations from the meeting and the decision makers for each.

4.6.5 Conduct Weekly In-Progress Reviews (IPR)

Conduct a Weekly In-Progress Review to discuss program, project and service status, existing or

potential problems, and projected tasks and milestones. In addition, the contractor shall provide updates to the PMP at the IPR. The contractor shall participate, document, and distribute minutes of regularly scheduled weekly status report meetings. The contractor shall meet with the Government Program Manager to discuss technical matters, share ideas, review milestones, activities accomplished, new and current issues and work progress. In addition, discuss and work out any outstanding administrative or managerial issues.

4.6.6 Transition Plans

4.6.6.1 Transition-in Plan

The Contractor must submit a transition plan that includes: How the Contractor will transition the work from the incumbent; a timeline showing the key steps to the transition process; amount of time proposed for the transition period; and any additional information the Contractor believes to be important.

The Contractor shall keep the Government fully informed of status throughout the transition period. Throughout the transisition-in period, it is essential that attention be given to minimize interruptions or delays to work in progress that would impact the mission. The Contractor must plan for the transfer of work control, delineating the method for processing and assigning tasks during the transition-in period.

4.6.6.2 Transition-out Plan

The Transition-Out Plan shall be due sixty (60) calendar days prior to the expiration date of the Order. Upon Government approval, the contractor shall implement its Transition-Out Plan. Prior to the end of the period of performance the contractor shall begin to transition all data, information, training material, all deliverables, etc., to the office (either Government or contractor) to perform the tasks in the PWS.

4.6.7 Orientation/Post Award

4.6.7.1 The Contractor shall participate in a Kick-Off Meeting/Conference Call with the Government at a time and place scheduled through the GSA acquisition team. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved with the call. The meeting will provide the opportunity to discuss technical, management, and security issues, as well as travel authorization, invoicing, and reporting procedures. At a minimum, the attendees shall include key contractor personnel, the client COR and other representatives from the client agency and participants representing the General Services Administration (GSA) Contracting Activity. The GSA Acquisition Team will lead the kick-off meeting. The Contractor shall keep the meeting minutes and submit them to the GSA acquisition team for review, with a copy to the client COR, due within five (5) working days. The agenda will include the following:

- Introductions of all parties, specifically decision makers

- Contractor personnel shall be prepared to introduce key personnel and their roles and responsibilities
- Overview of Order
- Contract administration
- Communication
- Travel/Non-Travel ODCs (if applicable)
- Performance Monitoring
- Deliverables
- Invoicing

4.6.7.2 Within ten (10) days of award the Contractor shall conduct an orientation briefing for the Government, apart from the kick-off meeting; however, if convenient to all parties, the Contractor may coordinate, with the GSA acquisition team, to schedule the orientation briefing to immediately follow the kick-off meeting. If the orientation briefing needs to be scheduled for a different time, the Contractor shall schedule the Orientation Briefing, to include the client agency and the GSA PM, for a mutually convenient date and time. The intent of the briefing is to initiate discussions between the client technical team and contractor project management team regarding the contractor's approach to accomplishing the technical tasks addressed in the PWS and to identify project priorities to facilitate full contractor performance. The contractor shall address updated transition-in plan milestones. The contractor shall submit the meeting notes to the client COR, with a copy to the GSA PM, for review and acceptance.

5.0 DELIVERABLES

Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

All deliverables shall be submitted to a designated area in DMDC's SharePoint. The Monthly Status Report shall also be submitted to GSA's IT Solutions Shop (ITSS) per PWS 4.6.1. Deliverables are not required to be emailed to GSA.

The general quality measures, set forth below, will be applied to each deliverable received from the Contractor under this contract:

- Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.
- Specifications Validity – All Deliverables must satisfy the requirements of the Government.
- File Editing – Where directed, all text and diagrammatic files shall be editable by the Government.

- Format – Deliverables shall follow DMDC guidance. Where none exists, the Contractor shall coordinate approval of format with the COR.
- Timeliness – Deliverables shall be submitted on or before the due date specified.

The Government will provide written acceptance, comments and/or change requests, if any, within fifteen work days from Government receipt of the draft deliverable. Contractor shall revise drafts and deliver finals within 5 work days of receipt of Government comments on draft, unless noted otherwise below. "Days" represents work days, unless otherwise noted. The work products and reports shall be delivered in accordance with dates listed in the following table:

Deliverable	SOW Reference	Due Date
Integrated Master Plan (IMP)	4.1.1	Draft submitted within thirty work days of start of performance; Final submitted within ten days after receipt of Government comments. Updates no less frequently than annually.
Work Breakdown Structure (WBS)	4.1.2	10 days after award
Decision Log	4.1.3	5 days after award
Maintained Collaboration or SharePoint sites	4.1.4	Updated 5 days after start of performance and updated within 2 days after documents change
Meeting Summaries	4.1.5	Within 3 business day of the meeting/teleconference
Project Documentation	4.1.6	30 days after start of performance and updated within 2 days after documents change
DMDC Governance approvals	4.1.7	Per Government approved IMP
SW Maintenance & Development Plan	4.2.1	15 days after award
System Security Plan	4.3.16.1	30 days after award

IA Vulnerability Remediation	4.3.16.2	Ongoing. Remediate IAVMs within the timeframe stipulated by DMDC Cybersecurity Branch
Continuous Monitoring Security Controls Assessment Schedule	4.2.16.4	Within 30 days of award
Plan of Actions and Milestones (POAM)	4.2.16.5	Within the timeframe stipulated by DMDC Cybersecurity Officer
IT Contingency Plan	4.3.16.10	60 days after award, with annual review/updates
COOP Tabletop Exercise After Action Report	4.5.10.3	Within five (5) days after exercise
Engineering Change Proposals (ECP)	4.3.18	Within thirty (30) days of receipt of request
Interface Requirement Specifications (IRS)	4.3.19.1	Within thirty (30) days of Production Readiness Review (PRR) for new development activities.
Interface Design and Description (IDD)	4.3.19.2	Within thirty (30) days of PRR for new development activities.
Software Product Specification (SPS)	4.3.20.1	Within thirty (30) days of PRR for new development activities.
System Subsystem Specification (SSS)	4.3.20.2	Within thirty (30) days of PRR for new development activities.
System/Subsystem Design Description (SSDD)	4.3.20.3	Within thirty (30) days of PRR for new development activities.
Database Design Description (DBDD)	4.3.20.4	Within thirty (30) days of PRR for new development activities.
Release Notes	4.3.21	Draft 5 days prior to testing Final 5 days prior to production implementation.

Software Maintenance & Development Plan (SMDP)	4.2.1.16	Within thirty (30) days of award
Requirements Traceability Matrix (RTM)	4.2.1.15	Within ten (10) days of PRR; update as appropriate to reflect changes
Requirements Versioning Tool	4.3.10	Within six (6) months after award
Software Version Description (SVD)	4.2.2.9	At the PRR milestone.
Test Environments	4.2.1.14	Per approved IMP and no later than date of assumption of full responsibiltity for operation of DTS
Software Test Description (STD)	4.2.3.4	15 days prior to Test Readiness Review (TRR) milestone for new development activities.
Software Testing Report (STR)	4.2.3.5	Within ten (10) days of completion of contractor testing.
Data Pulls	4.3.14.1	Within 5 business days of request; or, for data pulls expected to require longer than 5 days, a delivery date within 24 hours of the request, followed by the report on the approved date.
Ad-Hoc Queries	4.3.14.2	Recurring monthly data pulls should be completed with 3 working days of request, provide a delivery schedule to the government within 24 hours for reports expected to take longer than 3 days
Automation of Recurring Reports	4.3.14.3	12 months from award
Compliance Audit Support Plan	4.3.15.2	Within ninety (90) days of award; annual review/updates

Hosting Migration Plan (GFE)	4.5.1	Preliminary Hosting Migration Plan within thirty (30) days after notification of hosting site relocation. Final Hosting Migration Plan within sixty (60) days after notification of hosting site relocation.
Outages Schedule	4.5.3.2	Per Government approved IMP
Operational Metrics Reports	4.5.5 4.5.13.9	Daily
Hosting Configuration Management Plan	4.5.7.1	30 days after award
Configuration Audit Plan	4.5.8.1	Per Government approved IMP
Rollback Plan	4.5.9	45 days after award
COOP Exercise & After Action Report	4.5.10.3	Annually, if exercised
Disaster Recovery Plan	4.5.10.4	30 days after award
Software Quality Performance Reports (SQPR)	4.3.15.10	Thirty (30) days after software release of new system functionality.
Hosting Transition-Out Plan	4.5.12	4 months prior to transition
Monthly Status Report (MSR)	4.6.1	MSR brief shall be held on the fifteenth (15) calendar day of each month; electronic copy of the MSR shall be delivered 3 days prior to the brief
Communication Plan	4.6.2	30 days after award
Problem Notification Report	4.6.3	3 days after identification of problem
Meetings/Trip Reports	4.6.4	5 days after completion of travel
In-Progress Review (IPR)	4.6.5	Weekly - Written report is due 1 day prior to meeting
Transition In Plan	4.6.6.1	Updated plan 10 days after award; updated Monthly until Contractor assumes full responsibility for DTS.

Transition Out Plan	4.6.6.2	60 work days prior to end of period of performance
Orientation/Post Award	4.6.7	Within 10 days after order award
Quality Control Plan	5.1	Draft submitted within 15 days of the start of performance, updated monthly per integral Quality Status Reports.
Risk Management Plan	5.3	Draft submitted within 15 days of the award
Non-Disclosure Agreements	5.9	Prior to any contractor personnel reporting for work
GFE/GFI list report	6.5	30 days prior to end of contrct

5.1 Quality Control Plan (QCP)

5.1.1 Establish a quality element that ensures compliance with applicable Federal mandates, contractual performance standards, and industry best practices. Consider as part of its Quality Control Plan (QCP) a number of standard approaches toward quality such as the International Standards Organization (ISO) and Systems Engineering Institute/Capability Maturity Model (SEI/CMM) processes.

5.1.2 Maintain a thorough quality control program with the aim of identifying and correcting deficiencies in the quality of services before performance becomes unacceptable. Develop a Quality Control Plan (QCP) that describes the Contractor's procedures for monitoring performance. The COR will notify the Contractor, in writing, of deficiencies in the plan and allow 5 working days for a revision to be submitted. At a minimum, the Quality Control Plan shall include the following:

5.1.2.1 Develop and maintain an inspection system that encompasses all requirements of the order. The inspection system shall satisfy the requirements within this PWS and shall be designed to keep the contractor's management informed of all issues affecting quality.

5.1.2.2. Quality Status Reports (QSRs) shall be generated on a monthly basis. Details of audits and inspections accomplished, significant deficiencies noted, trend analysis of order performance and current status of all issues yet to be resolved (dealing with the particular module/phase which is under development during that time frame). QSRs shall be distributed to the contractor's program management and Government representatives concurrently. At a minimum, the QSRs must include metrics, which verify whether the performance standards in the PWS have been met.

5.1.2.3. The QC function shall ensure that timely and effective corrective action is obtained for all deficiencies identified by the Government. All deficiency responses shall include identification of the cause of the deficiency (if the software "bug" is known at the time of inspection).

5.1.2.4. The contractor may be required to conduct special inspections at the contracting officer's representative written request. Results of the inspection or audit shall be provided, in writing, in a timely manner as determined by the COR.

5.1.2.5. Develop the QCP based on accepted industry standards and detail the processes, procedures, and metrics for assuring quality. The QCP shall also include establishment of capable processes; monitoring and control of critical processes and product variation; establishment of mechanisms for feedback of field performance

5.2 PERFORMANCE STANDARDS

The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation. It should be understood that failure to meet the performance metrics below will result in negative past performance evaluations.

Past Performance Evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations will contain detailed narratives explaining reasons for positive and negative assessments. The following are the specific performance standards for this PWS.

Performance Standard	Acceptable Quality Level (AQL)	Method of Surveillance
System Availability	(excluding unavailability attributable to the directed subcontracting hosting contractor) DTS is available to users a minimum of 98.5% based on a 24x7 basis measured monthly. This includes network availability and connectivity to external DTS interfaces and applies to CDC 1 and CDC 2 facilities.	- Actual system uptime/(total available uptime-Government approved downtime) - Contractor delivered reports as defined in PWS - Review of maintenance and network event tracking logs
Deliver software/services on time, on budget, and right the first time (Per DMDC SDLC)	Timeliness: On time in accordance with Project Timeline, desired to have a decreasing trend. Quality: The release works as	Calculation: Projects delivered on time / total projects delivered over the rolling last 12 calendar-months Data Source: Official Project Schedules. Calculation 1: Total number of

	expected per the RTVM, desired to have a decreasing trend.	bugs found in Contractor Test that escaped through the QA testing over the rolling last 12 calendar-months Calculation 2: Total number of bugs found in Production that escaped through the QA testing over the rolling last 12 calendar-months Data Source: Defect tracking tool.
Software/service quality (Per DMDC SDLC)	Change Efficiency: How efficiently are we handling changes – are we working our backlog down? Desired upward trend. Release Quality: How good is the release (software/service and documentation) delivered for deployment to Production? Desired upward trend.	Calculation: Total number of changes implemented / total number of changes scheduled for implementation over the rolling last 12 calendar-months Data Source: Change Tracking Tool Calculation: Total number of software/service releases that deployed successfully the first time / the total number of deployments over the rolling last 12 calendar-months Data Source: Change/defect and incident management tracking tools
SDLC Process was followed (Per DMDC SDLC)	Number of vulnerabilities How efficiently are we handling changes – are we working our backlog down? Desired downward trend.	Calculation: Total number of open vulnerabilities in Production software/services (minus) total number of vulnerabilities over the rolling last 12 calendar-months Data source: Cyber hardening POA&Ms for software/services
DTS Application Performance	DTS application hourly average web page response time does not exceed 2 seconds during	-Daily performance reports as defined in Operational Metrics

	any hourly increment of any day on CDC 1	
Real Time Approved Transactional Data shall have 0% data loss	0% Approved Transactional data loss during failover to CDC 2 DR/COOP facility	Government review/inspection
Sustainment SPR fixes do not introduce new SPRs	No new defects shall be introduced into the system due to a sustainment SPR fix	Travel Assistance Center (TAC) Tickets, customer feedback, Technical Review Team (TRT) input and SPR reports
Government acceptance	No Priority 1 (P1) or Priority 2 (P2) SPR's at Government acceptance	100% government review and inspection (physical or paperwork)
Government acceptance of documentation artifacts	Documentation complies with best practices and standards set by the Government, and meets or exceeds requirements	Government review and inspection
Functionality of the software to meet required systems architecture and processing capabilities	Functionality defined in the requirements must be prioritized and tolerances for deviation assigned for each component. 95% of operational capability is acceptable, as determined by the Qualit Control Plan.	Independent verification & validation (IV&V) for testing new releases of software to determine that previous functionality is maintained. Customer satisfaction as measured through limited validated customer complaints, feedback, and surveys. For conversion projects, independent verification & validation (IV&V) for developing or maintaining system processing/benchmark during parallel processing.
Delivery dates are met, or exceeded	99% compliance	100% inspection
Meet all Government and agency specific requirements	100% compliance	100% inspection to ensure that all Government and Agency specific requirements have been met. Independent verification of security procedures-defined by agency (could be

		performed by a third party or another agency according to current security regulations and measures.
Software adds value and improves existing functionality without negatively impacting the existing operational environment.	Base line functionality is met at 100%. Non critical functionality is met at 80%	Independent Verification and Validation (IV&V) for testing new releases of software to determine that previous functionality is improved. Customer satisfaction is measured through validated customer complaints and surveys.
Integrated Master Plan	100% of areas required by government including the WBS are created and updated monthly. 95% On time delivery of Initial and Monthly Updates	100% Inspection
Quality Control Plan	99% On time delivery of Initial and Monthly Updates	Random Monitoring and Partial Inspection Quarterly by COR
Risk Management Plan (RMP) RMP delivered on-time and updated monthly	100% on time delivery of initial RMP 95% delivery of updates by last workday of each month.	Routine inspection of deliverable products and services.
Support Service Staffing: Personnel possess necessary knowledge, skills, and abilities to perform tasks in accordance with the PWS and the skill set of the labor category quoted and accepted at order award	Satisfactory or higher	CPARS/COR Observation/Customer assessments
Release and Production Drop Schedules	Schedules consistently depicted well-planned, staged and sequence activities. Schedules made optimal use of the resources.	Schedules reviewed at the Weekly IPR Explanation of scheduled and unscheduled changes shall be provided during regularly

	Flexibility and decisions making showed a consistent ability to promptly identify, evaluate, react and incorporate, into planning and implementation issues as they relate to meeting release and production schedules.	scheduled IPR Observation of Key Govt POCs
Customer Satisfaction	Provides value-added advice/thought leadership and deliverables that reflect the DMDC's needs to achieve program success 99% satisfaction	Help desk surveys, Annual Past Performance Evaluation
Responsiveness	Responds to staff and acknowledges inquiry within one business day 99% of all inquiries are responded to	Direct Observation

5.2.1 Customer Complaint Surveillance. This action is instituted when the COR receives a complaint from a stakeholder regarding contractor service. The COR will obtain the complaint in writing and then conduct an investigation to determine its validity. If the complaint is deemed valid, the COR will immediately notify the Contracting Officer for action. The COR will notify both the Contracting Officer and the complainant of the Government's response to their complaint.

5.2.2 Contract Discrepancy Report (CDR). In the event of unsatisfactory contractor performance, the COR or CO will issue a CDR that will explain the circumstances and findings concerning the incomplete or unsatisfactory service. The contractor shall acknowledge receipt of the CDR and respond in writing as to how he/she shall correct the unacceptable performance and avoid a recurrence. The Government will review the contractor's corrective action response to determine acceptability and will use any completed CDR as part of an overall evaluation of Contractor performance when determining present or future contractual actions.

5.3 Risk Management Plan

The Contractor shall assess, evaluate, document, and manage risks associated with the performance of this order and create, modify, maintain, and implement a Risk Management Plan.

5.4. Records/Data
The contractor shall deliver to DMDC all software, software licenses, data, form, fit and data first produced (including source code), written documents, technical data, software developed, and infrastructure designed and reports to include, at a minimum, system change plans, various operations procedures and planning documents, meeting minutes, reports, manuals, training text, program management reviews, financial status reports, and any other documents created in support of this order. All system documentation shall be updated to remain current with each software development activity/phase. DMDC will have unlimited rights as allocated under FAR 52.227-14(b) in all data delivered under the order. Unless otherwise stated in the order, the contractor shall submit deliverables to the COR or his or her designee. The COR will serve as DMDC's focal point for accepting the deliverables unless the order provides for other procedures.

Clauses DFARS 252.227-7013 & DFARS 252.227-7014 are hereby incorporated.

5.5. Limited Use of Data
Performance of this effort may require the Contractor to access and use data and information proprietary to a Government agency or Government Contractor which is of such a nature that its dissemination or use, other than in performance of this effort, would be adverse to the interests of the Government and/or others. Contractor and/or Contractor personnel shall not divulge or release data or information developed or obtained in performance of this effort, until made public by the Government, except to authorize Government personnel or upon written approval of the Contracting Officer (CO). The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the performance of this effort. Nothing herein shall preclude the use of any data independently acquired by the Contractor without such limitations or prohibit an agreement at no cost to the Government between the Contractor and the data owner which provides for greater rights to the Contractor.

5.6. Disclosure of Information
Information made available to the Contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other way without the written agreement of the Contracting Officer. The Contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information. Each Contractor or employee of the Contractor to whom information may be made available or disclosed shall be notified in writing by the Contractor that such information may be disclosed only for a purpose and to the extent authorized herein.

5.7. Contractor Identification
All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. Electronic mail signature blocks shall identify contractor/company affiliation. They must also ensure that all documents or reports produced by contractors are suitably marked as

contractor products or that contractor participation is appropriately disclosed. Contractor personnel occupying collocated space in a Government facility shall identify their workspace are with their name and company/contractor affiliation.
All Contractor staff that have access to and use of the Government electronic mail (e-mail) shall identify themselves as contractors on all outgoing e-mail messages, including those that are sent in reply or are forwarded to another user. To best comply with this requirement, the contractor staff shall set up an e-mail signature ("AutoSignature") or an electronic business card ("V-card") on each contractor employee's computer system and/or Personal Digital Assistant (PDA) that will automatically display "Contractor" in the signature area of all e-mails sent. All work performed shall be conducted using government provided email. Personal or company email shall not be used to perform government work.

5.8. Organizational Conflict of Interest
Contractor and subcontractor personnel performing work under this order may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.), or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

5.9. Non-Disclosure Requirements
All contractor personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the Order issued which requires the contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and submit a Contractor Non-Disclosure Agreement" Form. This is required prior to the commencement of any work on such order and whenever replacement personnel are proposed under an ongoing order. Any information obtained or provided in the performance of this order is only to be used in the performance of the order. The Contractor shall take the necessary steps in accordance with Government regulations to prevent disclosure of such information to any party outside the Government and to indoctrinate its personnel who have access to sensitive information and the relationship under which the Contractor has possession of or access to the information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information will be used for the profit of any party other than those furnishing the information. The Nondisclosure Agreement for Contractor Employees shall be signed by all indoctrinated personnel and forwarded to the Contracting Officer Representative (COR) for retention, prior to work commencing. The Contractor shall restrict access to sensitive/ proprietary information to the minimum number of employees necessary for order performance.

5.10 Cooperation with Other On-Site Contractors
When the Government undertakes or awards other orders or contracts for additional work the Contractor will: (1) fully cooperate with the other Contractors and Government employees, and (2) carefully fit its own work to such other additional contracted work as may be directed by the Contracting Officer's Representative (COR). The Contractor shall not commit or permit any act that will interfere with the performance of work awarded to another Contractor or with the performance of other Government employees. In any case where, in the course of fulfilling the order requirements, the Contractor disturbs any work guaranteed under another separate contract, the Contractor shall restore such disturbed work to a condition satisfactory to the COR and guarantee such restored work to the same extent as it was guaranteed under the other contract.

5.11 Training Requirements For Government Contractors (5 CFR 930.301(1))
If contractors use Government computers, they shall complete DMDC-sponsored IT Security Awareness training. Other DMDC mandated training courses include:

- Records Management
- Insider Threat
- Environmental Management System (West cost only)
- Information assurance (IA)/Cyber Awareness Challenge Training
- Privacy act and Personally Identifiable Information (PII) (combined)
- Civil Liberties
- Counter Intelligence (CI) Awareness

5.12. Data Rights
The Government requires unlimited rights in any technical data, software developed, and infrastructure designed first produced in the performance of this order, in accordance with the FAR clause at 52.227-14. In addition, for any technical data, software developed, and infrastructure designed first produced in the performance of the order, the technical data, software developed, and infrastructure designed may be shared with other agencies or contractors during the period of performance of the order, or after its termination. For any subcontractors or teaming partners, the Contractor shall ensure at proposal submission that the subcontractors and /or teaming partners are willing to provide the data rights required under the order.

5.13. KEY PERSONNEL

Key personnel are personnel who are integral and indispensable in completing a contract/call order. Key personnel shall be available at contract/project start, with the exception of the contract/order Manager, who shall be available immediately after award. The following are the minimum personnel who shall be designated as “Key.” The Government does not intend to dictate the composition of the ideal team to perform this TO. The contractor may designate additional “Key Personnel”.

a. Project Manager (PM)

b. Chief Engineer
c. Information Assurance Specialist

The Government desires that Key Personnel be assigned for the duration of the TO.

Program Manager/Project Manager

The Project Manager must hold a Project Management Professional (PMP) certification or other equivalent/recognized Project Management certification and maintain a Secret Security Clearance, IT Level 3 Investigation, and demonstrated experience in all of the following areas:

- Project Management Professional (PMP) certification.
- Experience in Project Management in IT environment (10 years) managing large-scale Information Technology programs
- 5+ years of DoD travel experience

The Program Manager/Project Manager is expected to split their time somewhat equally between the contractor's site and the DTS office in the Mark Center.

Chief Engineer

The Chief Engineer shall have a Secret clearance prior to starting work on this Task Order. A higher clearance is acceptable. It is desirable that the Chief Engineer has the following qualifications:

- Extensive experience in System Engineering
- Five plus years of DoD travel Experience
- Experience in Information Technology engineering processes.
- Experience with large scale Federal Information Technology projects.

Information Assurance Specialist

The Information Assurance Specialist shall have a Top Secret clearance prior to starting work on this Task Order. The Information Assurance Specialist shall have a current Certified Information Systems Security Professional (CISSP) Certification. It is desirable that the Information Assurance Specialist has the following qualifications:

- Experience in evaluating and implementing Information Assurance tools for assessing and maintaining system security within the Defense Information Infrastructure (DII) to support system development and integration.
- Knowledge and experience performing appropriate analyses to ensure threat assessments, protection, detection, and reaction functions are performed.
- Knowledge and experience managing or implementing DOD information security, communications-computer systems security and industrial security policies and procedures.

- Knowledge and experience training information systems personnel on DOD security policies and procedures.
- Knowledge and experience developing standardized certification and authorization processes in accordance with RFM policy and maintain established authorization baselines.

6. ADMINISTRATIVE CONSIDERATIONS

6.1. Points of Contact

6.1.1. Client Contracting Officer's Representative (COR)

Pamela Bridges
Defense Manpower Data Center
(831) 583-4044
pamela.r.bridges.civ@mail.mil

6.1.2. GSA Project Manager/Contracting Officer's Representative (PM/COR)

Wesley Mellon
GSA Federal Acquisition Service (Mid-Atlantic Region)
Assisted Acquisition Service (3QFAA)
100 S Independence Mall W
Philadelphia, PA 19106-2320
Voice: 215-446-4566
wesley.mellon@gsa.gov

6.1.3. GSA Contract Specialist (CS)

Anthony Giannopoulos
GSA Federal Acquisition Service (Mid-Atlantic Region)
Acquisition Operations Division (3QSBC)
100 S Independence Mall W
Philadelphia, PA 19106-2320
Voice: 215-606-1761
anthony.giannopoulos@gsa.gov

6.1.4. GSA Contracting Officer (CO)

Ryan Schrank
GSA Federal Acquisition Service (Mid-Atlantic Region)
Acquisition Operations Division (3QSBC)
100 S Independence Mall W
Philadelphia, PA 19106-2320
Voice: 215-446-2853
Ryan.schrank@gsa.gov

6.2 HOURS OF WORK/PLACE OF PERFORMANCE

The contractor is responsible for conducting business, between the hours of 8 a.m. to 5 p.m., Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons.

Place of Performance is the contractor's facility (and the DTS offices for the Program Manager/Project Manager in Mark Center, Alexandria, VA). Some long distance travel is anticipated to be required in support of this effort.

6.3 PERIOD OF PERFORMANCE

The period of performance for this task order is a one-year base period and four, one-year options, beginning September 24, 2018, or date after receipt of award Anticipated Periods of Performance are:

Base Year- September 24, 2018 through September 23, 2019
Option Year 1 - September 24, 2019 through September 23, 2020
Option Year 2 - September 24, 2020 through September 23, 2021
Option Year 3 - September 24, 2021 through September 23, 2022
Option Year 4 - September 24, 2022 through September 23, 2023

The Contractor shall assume comprehensive operational responsibility for the DTS no later March 24, 2019.

6.4 TRAVEL

The Government anticipates that travel to the DMDC Mark Center offices, and other locations, may be required during the performance period. Exact locations and frequency are unknown at this time. Specific locations, dates and personnel required, etc., shall be identified by DMDC during task performance. It is anticipated that trips will include travel to attend meetings and to support performance.

The Not-To-Exceed dollar value established for Travel is $30,000.00 per performance period. This Travel ceiling shall not be exceeded without the advanced written approval of the GSA Contracting Officer.

All travel shall be pre-approved by the Project Manager and fully coordinated with the client COR prior to conducting the travel to ensure that funding and approvals are obtained before incurring any travel costs. Reimbursement shall include full travel costs and per diem reimbursement consistent with the Federal Travel Regulations, and reimbursement of general and administrative expense, as appropriate. Where feasible, the Contractor will use teleconferencing and electronic media transfers of data as much as possible to limit travel costs. The Contractor will seek the least expensive form of travel as is practical to the fulfillment of the performance of the Call.

In accordance with FAR 31.205-46, travel costs are to be reimbursed at rates not to exceed the maximum locality per diem rates (the combination of lodging, meals and incidentals) in effect at the time of travel, as set forth in the Federal Travel Regulations, Joint Travel Regulation and Standards Regulations, Section 925, as applicable. All air travel must be booked on American flagged carriers, unless otherwise directed by the Contracting Officer. All invoices for travel reimbursement shall be accompanied by supporting receipts.

6.5 GOVERNMENT FURNISHED EQUIPMENT (GFE)

The Government will provide office supplies, and computer and software resources at DMDC Seaside, CA and the Mark Center, VA, if applicable. The contractor has the primary responsibility for exercising reasonable care and control of GFE in its possession, or usage. Responsibility for reasonable care and control of GFE provided under the order in the possession of a subcontractor remains with the prime contractor. The contractor may be liable for damages, shortages of GFE when it is disclosed that the equipment is lost, damaged, or destroyed. GFE must be used only for the purposes set forth in this order.

Upon request of the Government, all Government furnished items shall be returned to the Government. All equipment or items furnished to the contractor shall be surveyed and a GFE/GFI list report shall be delivered to the COR at end of the order.

6.6 GOVERNMENT FURNISHED INFORMATION (GFI)

The Government will provide the following information: access to relevant Government organizations, information and documentation, manuals, texts, briefs, and associated materials as required and available. Access will be granted to classified networks under the guidance of the appropriate Government Security Manager.

6.7 ENTERPRISE-WIDE CONTRACTOR MANPOWER REPORTING APPLICATION (ECMRA)

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for SPORTS via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil. Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2013.

7. SECURITY

Contractor shall maintain Personnel Security Program in accordance with current DODD 5200.2. Contractor personnel requiring access to DTS shall have background investigations and must have completed privacy and security awareness training prior to accessing DTS. When contractor personnel are terminated from the project, System Administrators shall immediately disable the account and have seventy-two (72) hours to remove accounts required for system/network access. All access cards and identification badges will be returned to COR.

The contractor shall fully staff this order in accordance with its awarded level-of-effort on the task order start date. The contractor shall ensure all personnel, assigned to perform the work of this requirement, are eligible for a Common Access Card (CAC), have Public Trust Clearances and a current investigation in place before they start work on this order.

Contractor shall comply with CyberSecurity requirements as outlined at Appendix F. Order of precedence in the case of any conflicting CyberSecurity requirements is Appendix F, then the base PWS.

DD Form 254, Contract Security Classification Specification will be incorporated into the order.

7.1. Security Clearance Requirements

Contractor personnel requiring access to classified information shall obtain the appropriate security clearance. The Government is not responsible for processing Contractor personnel for national security clearance (SECRET). The contractor shall comply with required DMDC personnel security requirements as specified by the Cybersecurity Branch. Interim Clearances will be reviewed upon notification to DMDC Information Security Branch. It is the responsibility of the contractor Facility Security Officer (FSO) to notify DMDC immediately if there is a change in clearance eligibility. If at any time, any contractor FSO is unable to obtain/maintain an adjudicated Personnel Security Investigation (PSI), the Contractor shall immediately notify the DMDC Cybersecurity Branch and remove such person from work under this order.

Resouces filling the following functional roles require Top Secret clearances:

- Database Administrator (DBA)
- System Administrator
- Developer

7.2. CAC Requirements

7.2.1. Contractor personnel with access to DMDC systems or data must comply with HSPD-12 Personal Identity Verification (PIV) issuance requirements, known as the Common Access Card (CAC) for DMDC and must be CAC or PIV ready prior to beginning work on this order:

7.2.1.1. All Contractor personnel must obtain/maintain a favorable FBI National Criminal History Check (fingerprint check)

7.2.1.2. Provide two forms of identity proofed identification (I-9 documents)

7.2.1.3. Be citizens of the United States

7.2.1.4. Submit a Standard Form (SF) 86 National Security Questionnaire through e-QIP that is favorably accepted by the Office of Personnel Management (OPM) for those:

- Who do NOT have an active security clearance
- Will be obtaining a position of trust through DMDC or
- Have NOT been favorably adjudicated within the last 24 months.

7.2.1.5. Background investigation has been scheduled by OPM.

7.2.1.6. Maintain favorable FBI National Criminal History checks and ensure completion and successful adjudication as required for Federal employment

7.2.1.7. Obtaining CAC or PIV ready status is the responsibility of the Contractor. It is the responsibility of the Contractor to notify DMDC when this is complete

7.3. Position of Trust Requirements

7.3.1. All Contractor personnel with access to DMDC systems or data must comply with DOD Personnel Security Program.. All persons on this contract will be designated in a Critical-Sensitive, or Non-Critical Sensitive position (IT-I or IT-II) as determined by the Government per position responsibilities. All enterprise wide system administration support, to include the mainframe support services will require IT-I. Prior to beginning work on this contract, the contractor will complete all required personnel security requirements as specified by Defense Human Resource Agency, Personnel Security Office.

7.3.2 Complete and submit a vetting application (Standard Form (SF) 86 National Security Questionnaire through e-QIP, fingerprints and proof of US citizenship) that is favorably accepted by the Office of Personnel Management (OPM) for all employees under this contract requesting a position of trust determination.

7.3.3. It is the responsibility on the contractor to ensure their employees and sub-contractors (if applicable) comply with DHRA personnel security requirements.

7.4 LAN Access Requirements

The Contractor shall comply with account access requirements as specified by the DMDC Cybersecurity Branch. At minimum:

7.4.1. Standard User LAN access at minimum require:

- a. Completed DMDC personnel security requirements.
- b. Complete DD 2875 Form(s) for all access required.
- c. Submit proof of completion for Personally Identifiable Information (PII) Training.
- d. Submit proof of completion Cyber Awareness Challenge Training.

- e. Adhere to and sign the DMDC Information Systems User Agreement(s).

7.4.2. Privilege User LAN access at minimum require:

- a. Completed DMDC personnel security requirements.
- b. Complete DD 2875 Form(s) for all access required.
- c. Submit proof of completion Privilege User Cyber Awareness Challenge Training.
- d. Adhere to and sign the DMDC Privilege Information Systems User Agreement(s).
- e. DoD 8140.01, Cyberspace Workforce Management certification.
- f. Computing Environment (CE) certification(s).

7.5 Information Assurance Requirements

7.5.1. The Contractor and all Contractor personnel with access to or responsibility for nonpublic Government data under this contract shall comply with DoD Directive 8500.1 Cybersecurity, , DODI 8510.01 Risk Management Framework, NIST 800-53, DoD Directive 5400.11 DoD Privacy Program, DoD 6025.18-R DoD Health Information Privacy Regulation, DoD 5200.2-R Personnel Security Program, and Homeland Security Presidential Directive (HSPD) 12.

7.5.2. The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of Government data. At a minimum, this must include compliance with DoDD 8500.01 and DoDI 8510.01 and provisions for personnel security and the protection of sensitive information, including Personally Identifiable Information (PII).

7.5.3. Contractor systems and information networks that receive, transmit, store, or process nonpublic Government data must be accredited according to DoDI 8510.01 Risk Management Framework and comply with annual Federal Information Security Management Act (FISMA) security control testing. All systems subject to RMF must present evidence of Assessment and Accreditation (A&A). Evidence of FISMA compliance must be presented in the form of a POA&M. The Contractor will be responsible for the cost of IA A&A and FISMA testing required for any Contractor owned and operated network, facility and/or application processing DoD information.

7.5.4 The Contractor shall ensure all media containing sensitive information (e.g., hard drives, removable disk drives, CDs, DVDs) considered for disposal will be destroyed. Prior to

7.5.4 The Contractor shall ensure all media containing sensitive information (e.g., hard drives, removable disk drives, CDs, DVDs) considered for disposal will be destroyed. Prior to destruction, media will be sanitized, i.e., all prudent and necessary measures shall be taken to ensure data cannot be retrieved through known conventional or unconventional means.

7.5.5 To the extent that the work under this contract requires the Contractor to have access to DoD sensitive information the Contractor shall after receipt thereof, treat such information as confidential and safeguard such information from unauthorized use and disclosure. The Contractor agrees not to

appropriate such information for its own use or to disclose such information to third parties unless specifically authorized by the Government in writing.

7.5.6 The Contractor shall allow access only to those employees who need the sensitive information to perform services under this contract and agrees that sensitive information shall be used solely for the purpose of performing services under this contract. The Contractor shall ensure that its employees will not discuss, divulge or disclose any such sensitive information to any person or entity except those persons within the organization directly concerned with the performance of the contract.

7.5.7 The contractor shall administer a monitoring process to ensure compliance with DoD Privacy Programs. Any discrepancies or issues should be discussed immediately with the COR and corrective actions will be implemented immediately.

7.5.8 The contractor will report immediately to the DMDC CIO / Privacy Office and secondly to the COR discovery of any Privacy breach. Protected PII is an individual's first name or first initial and last name in combination with any one or more of the following data elements: social security number; biometrics; date and place of birth; mother's maiden name; criminal, medical and financial records; educational transcripts, etc.

7.5.9 Government may terminate this contract for default if Contractor or an employee of the Contractor fails to comply with the provisions of this clause. The Government may also exercise any other rights and remedies provided by law or this contract, including criminal and civil penalties.

7.5.10. The Contractor is responsible for safeguarding all Government equipment, information and property. At the close of each work period, Government facilities, equipment, and materials shall be secured.

7.6. Classified Data Processing

Based on DoD Regulation 5200.2-R, some aspects of the tasking described in this PWS requires, at minimum, a SECRET Clearance, or a SECRET Clearance In Progress, for employees who support the classified systems and/or applications at DMDC. All documentation and cost for clearance processing shall be the responsibility of the contractor. Upon award, a DD Form 254 will be issued to the contractor. The Contractor must have an approved classified processing facility. All classified data processing must be completed in an approved classified processing facility. Approved classified processing facilities include: DMDC, Seaside, CA, and the Mark Center, , Alexandria, VA. Additional classified processing facilities may be identified within specific tasks.

7.7 Breach Response

DoD 5400.11-R, "DoD Privacy Program," May 14, 2007, defines a breach as the "actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected."

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with DFAR Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007. The contractor shall also comply with federal laws relating to freedom of information and records management. Upon discovery of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access, the contractor/subcontractor shall immediately and simultaneously notify the COR, the designated Cyber Security Officer, and Privacy Officer for the contract within one (1) hour. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to DMDC assets, or sensitive information, or an action that breaches DMDC security procedures.

The Contractor shall adhere to the reporting and response requirements set forth in the Office of the Secretary of Defense (OSD) Memorandum 1504-07, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," June 5, 2009; DoD 5400.11-R, and applicable DMDC Privacy Office guidance. The Contractor shall, at their own expense, take action to mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of Protected Information by the Contractor in violation of the requirements of this Clause.

8.0 Appilicable Standards

All work under this order shall comply with the latest version of all applicable standards. These may include, but are not limited to, DOD and DHRA Manual(s), Acquisition Bulletins [AB], American National Standards Institute [ANSI] standards, and National Institute of Standards and Technology [NIST] standards, including Federal Information Processing Standards [FIPS] publications. Software Development Standards Life Cycle (SDLC).

The contractor shall, over the term of this order, correct errors in Contractor developed software and applicable documentation that are not commercial off the shelf which are discovered by the Government, and any other user of the software, or the Contractor. If the system is in production, such corrections shall be completed within one working day of the date the Contractor discovers or is notified of the error (or a date mutually agreed upon between the CO and the Contractor not to exceed 30 working days). If the system is not in production, such corrections shall be made within five working days of the date the Contractor discovers or is notified of the error (or a date mutually agreed upon between the CO and the Contractor, not to exceed 30 days). Latent defects will be handled in the same manner, as soon as they are discovered. Inability of the parties to determine the cause of software errors shall be resolved in accordance with the Disputes clause in Section I, FAR 52.233-1, incorporated by reference in the contract, but in no event constitutes grounds for delay of error correction beyond the periods specified.

9.0 CLAUSES

See Appendix H.

10.0 APPENDICES

Appendix A – List of Government Furnished Hardware
Appendix B – List of Government Furnished Software
Appendix C – Network & System Interfaces
Appendix D – ECP Process
Appendix E – DMDC SW Development Process
Appendix F - Cyber Security Procedures
Appendix G - Currrent order Transition Out Plan
Appendix H - Clauses
Appendix x – (placeholder for to-be-provided DD Form 254)